INFORMATION AND CONTROL 19, 345–352 (1971)

On the Length of Feedback Shift Registers*

J. ROBERT JUMP AND SHREEHARI MARATHE

Laboratory for Computer Science and Engineering,
Department of Electrical Engineering, Rice University,
Houston, Texas 77001

A result relating the length of a feedback shift register to the lengths of the cycles in its state transition graph is presented. Specifically, it is shown that, if a state of a feedback shift register is in one cycle of length c_1, and another cycle of length c_2, then the length of this shift register must be less than $c_1 + c_2 - \text{g.c.d.}(c_1, c_2)$. This result is then shown to be relevant to the problem of realizing sequential machines with feedback shift registers.

1. INTRODUCTION

This paper is concerned with properties of feedback shift registers. In particular, the relationship between the length of the shift register and the lengths of the cycles in its state transition graph is studied. These properties are shown to be pertinent to the problem of realizing the state behavior of sequential machines with shift registers.

More specifically, it is shown that if a state of a feedback shift register is in two cycles of different lengths, then the length of that shift register cannot exceed the sum of the cycle lengths minus their greatest common divisor. Thus, the cycle structure of a sequential machine can be used to compute an upper bound on the length of certain feedback shift register realizations.

It is known that to realize a particular sequential machine as a feedback shift register, it may be necessary to replace certain states in its flow table with sets of equivalent states (state splitting). Several authors have developed algorithms for testing a machine to determine whether or not this is necessary. Typical of these are Davis (1968), Haring (1966), Johnson and O'Keefe (1968), Liu (1964), Martin (1969), and Nichols (1965). Most of these algorithms are iterative and must, in effect, try shift registers of increasing lengths

* This research was supported in part by the National Science Foundation under Grant No. GJ-750.

until either a realization is found or it is established that additional equivalent states must be used. For some machines, the results of this paper can be used to reduce the number of iterations which must be performed.

2. Definitions and Notation

In this paper, we are only concerned with properties of sequential machines that are independent of their outputs. We therefore model a *sequential machine* by an ordered triple $M = (Q, \Sigma, \delta)$, where Q denotes a finite nonempty set of *states*, Σ denotes a finite nonempty set of *input symbols*, and δ denotes the *state transition function* which maps $Q \times \Sigma$ into Q.

Given a sequential machine $M = (Q, \Sigma, \delta)$, we extend the state transition function to finite sequences of input symbols in the usual way. In particular, if $\bar{\sigma} = \sigma_1\sigma_2 \cdots \sigma_k$ is a sequence of k input symbols, then the *terminal state function* $\bar{\delta}$ is defined inductively as follows:

(1) if $k = 1$, then $\bar{\delta}(q, \bar{\sigma}) = \delta(q, \bar{\sigma})$, and

(2) if $k > 1$, then $\bar{\delta}(q, \bar{\sigma}) = \delta(\bar{\delta}(q, \sigma_1\sigma_2 \cdots \sigma_{k-1}), \sigma_k)$

for all q in Q.

We will say that a state q of a sequential machine $M = (Q, \Sigma, \delta)$ belongs to a cycle of length k if there is a sequence of k input symbols which takes the machine from state q back to itself without passing through any state more than once. Thus, q belongs to a cycle of length k if there is a sequence of input symbols $\sigma_1\sigma_2 \cdots \sigma_k$ such that

(1) $\bar{\delta}(q, \sigma_1\sigma_2 \cdots \sigma_k) = q$, and

(2) $\bar{\delta}(q, \sigma_1\sigma_2 \cdots \sigma_i) \neq \bar{\delta}(q, \sigma_1\sigma_2 \cdots \sigma_j)$ for $1 \leqslant i < j \leqslant k$.

A *feedback shift register* (FSR) is illustrated in Fig. 1. It consists of two parts, an ℓ-stage tapped delay line and a logic network. We do not restrict ourselves to binary delay lines but assume that each stage can store a symbol from some finite set S. The logic network can be viewed as a device for computing a function f from $S^\ell \times \Sigma$ into S, where Σ is a set of input symbols.

If we now represent the output signal of the i-th delay element at time t by the variable $s_i{}^t$ and the input signal at time t by σ^t, then the behavior of an FSR can be described by means of the following equations:

(1) $s_i^{t+1} = s_{i+1}^t$ for $i = 1, 2, \ldots, \ell - 1$,

(2) $s_\ell^{t+1} = f(s_1{}^t, s_2{}^t, \ldots, s_\ell{}^t, \sigma^t)$.

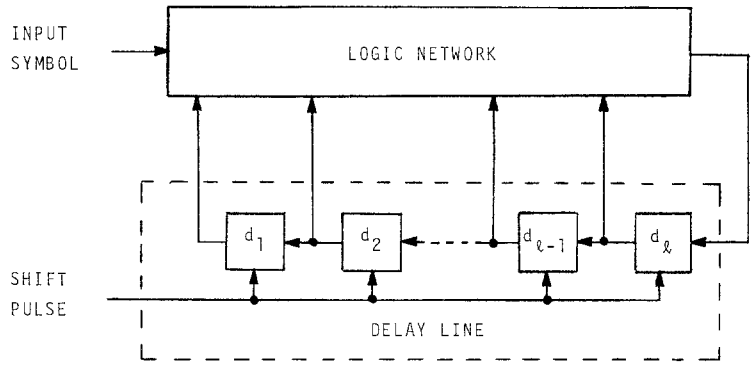

FIG. 1. Typical feedback shift register.

An FSR can therefore be viewed as a sequential machine $F = (S^\ell, \Sigma, \delta_f)$, where $\delta_f(s_1, s_2, \ldots, s_\ell, \sigma) = (s_2, s_3, \ldots, s_\ell, f(s_1, s_2, \ldots, s_\ell, \sigma))$.

We are interested in the problem of realizing the state transition behavior of a sequential machine $M = (Q, \Sigma, \delta)$ by means of an FSR. It is well known that this is equivalent to encoding the states of M with ℓ-tuples $(s_1, s_2, \ldots, s_\ell)$ of elements of some set S in such a way that

(1) no ℓ-tuple is assigned to more than one state;

(2) the last $\ell - 1$ elements of the ℓ-tuple assigned to the state q are the same as the first $\ell - 1$ elements of the state $\delta(q, \sigma)$, for all σ in Σ and q in Q.

We call such an encoding an *FSR assignment*. If every state has been assigned only one ℓ-tuple, then we say that the assignment is *one-to-one*.

Finally, we observe that if a sequential machine M is realized by an FSR, using a one-to-one assignment, then a state q of M belongs to a cycle of length k only if there is a state in the FSR which also belongs to a cycle of length k. Indeed, the state $(s_1, s_2, \ldots, s_\ell)$ assigned to q is such a state.

3. The Length of Shift-Register Realizations

In this section, we show how the cycle structure of a sequential machine is related to the length of delay lines which can be used to realize it. We begin with the following generalization of a property of autonomous feedback shift registers [Yoeli 1963].

THEOREM 3.1. *Let* $q = (s_1, s_2, \ldots, s_\ell)$ *be a state of an* FSR *of length* ℓ.

If q belongs to a cycle of length k, then $s_i = s_{i+k}$ for $i = 1, 2, \ldots, \ell - k$. Furthermore, if d is a positive integer which divides k and if $s_i = s_{i+d}$ for $i = 1, 2, \ldots, \ell - d$, then $d = k$.

Proof. Since q belongs to a cycle of length k, there is an input sequence $\bar{\sigma} = \sigma_1\sigma_2 \cdots \sigma_k$ such that

$$\bar{\delta}_f(q, \bar{\sigma}) = q = (s_1, s_2, \ldots, s_\ell)$$

and for no $j < k$ does $\bar{\delta}_f(q, \sigma_1\sigma_2, \ldots, \sigma_j) = q$. But

$$\bar{\delta}_f(q, \bar{\sigma}) = (s_{k+1}, s_{k+2}, \ldots, s_\ell, t_{\ell+1}, \ldots, t_{\ell+k}),$$

where $t_{\ell+1}, t_{\ell+2}, \ldots, t_{\ell+k}$ depend on the feedback function f. Equating components of these two ℓ-tuples, we see that $s_i = s_{i+k}$ for $i = 1, 2, \ldots, \ell - k$ which proves the first part of the theorem. We also note that $s_{\ell-k+i} = t_{\ell+i}$ for $i = 1, 2, \ldots, k$. In order to prove the second statement, assume that $k = md$ for some integers m and d greater than 1 and that $s_i = s_{i+d}$ for $i = 1, 2, \ldots, \ell - d$. Then, applying the first d symbols of $\bar{\sigma}$ to the shift register, we have that

$$\begin{aligned}\bar{\delta}_f(q, \sigma_1\sigma_2 \cdots \sigma_d) &= (s_{d+1}, s_{d+2}, \ldots, s_\ell, t_{\ell+1}, \ldots, t_{\ell+d}) \\ &= (s_1, s_2, \ldots, s_{\ell-d}, t_{\ell+1}, \ldots, t_{\ell+d}).\end{aligned}$$

But $t_{\ell+j} = s_{\ell-k+j} = s_{\ell-md+j} = s_{\ell-d+j}$ for $j = 1, 2, \ldots, d$. Hence,

$$\bar{\delta}_f(q, \sigma_1\sigma_2 \cdots \sigma_d) = (s_1, s_2, s_3, \ldots, s_\ell) = q$$

and $d < k$. But this contradicts the statement that q is in a cycle of length k under input sequence $\bar{\sigma}$. Q.E.D.

In order to relate the delay-line length to the cycle lengths, we will also need the following property of infinite periodic sequences.

THEOREM 3.2. *Let $\bar{x} = x_0x_1x_2 \cdots$ and $\bar{y} = y_0y_1y_2 \cdots$ be two infinite sequences such that*

(a) $x_i = x_{i+m}$ *for* $i \geqslant 0$,

(b) $y_i = y_{i+n}$ *for* $i \geqslant 0$, *and*

(c) $x_i = y_i$ *for* $0 \leqslant i < m + n - d$,

where m, n, and d are positive integers and d divides both m and n. Then, the two sequences are equal. Furthermore, if g is the greatest common divisor of m and n, then $x_i = x_{i+g}$ for $i \geqslant 0$.

Proof. Without loss of generality, we assume that the elements in these sequences are positive integers. We then let

$$X(\xi) = x_0 + x_1\xi + x_2\xi^2 + \cdots$$

and

$$Y(\xi) = y_0 + y_1\xi + y_2\xi^2 + \cdots$$

denote the generating functions of the sequences. We will show that

$$X(\xi) - Y(\xi) = 0.$$

Since $\bar{x}$ has period m, there is a polynomial $P(\xi)$ of degree at most $m - 1$ such that

$$X(\xi) = \frac{P(\xi)}{1 - \xi^m}.$$

Similarly,

$$Y(\xi) = \frac{Q(\xi)}{1 - \xi^n}$$

for some polynomial of degree at most $n - 1$. Now

$$X(\xi) - Y(\xi) = \frac{P(\xi)(1 - \xi^n) - Q(\xi)(1 - \xi^m)}{(1 - \xi^m)(1 - \xi^n)}.$$

It can be easily seen that $1 - \xi^d$ divides both $1 - \xi^m$ and $1 - \xi^n$ since d is a divisor of both m and n. Hence,

$$X(\xi) - Y(\xi) = \frac{A(\xi)}{B(\xi)}$$

where $A(\xi)$ is a polynomial of degree at most $(m + n - 1) - d$ and $B(\xi)$ is a nonzero polynomial of degree $m + n - d$.

Since $\bar{x}$ and $\bar{y}$ agree in the first $m + n - d$ positions, the first $m + n - d$ coefficients of the polynomial $X(\xi) - Y(\xi)$ are zero. Hence, the first $m + n - d$ coefficients of $B(\xi)(X(\xi) - Y(\xi)) = A(\xi)$ are also zero. But the degree of $A(\xi)$ is less than $m + n - d$ so that $B(\xi)(X(\xi) - Y(\xi)) = 0$. Since, $B(\xi) \neq 0$, $X(\xi) - Y(\xi) = 0$ so that $\bar{x} = \bar{y}$.

Finally, let g denote the greatest common divisor of m and n. Then, there are two integers a and b such that $g = am + bn$. Since a and b cannot both be less than 1, we assume that $a > 0$. Then,

$$x_i = x_{i+am} = y_{i+am} = y_{i+am+bn} = y_{i+g} = x_{i+g} \qquad \text{for all } i \geqslant 0.$$

Q.E.D.

The theorem states that if two sequences, one with period m and the other with period n, agree in their first $m + n - d$ positions and if d divides both m and n, then they must be equal. We note that $m + n - g$, where g is the greatest common divisor of m and n, is the least integer for which this result is valid. Indeed, consider the following two unequal sequences:

$$10101 \quad 10101 \quad 10101 \quad 10101 \cdots$$
$$1010110 \quad 1010110 \quad 1010110 \cdots$$

The first has minimum period 5 and the second has minimum period 7 and they agree in the first $m + n - g - 1 = 10$ positions.

Finally, we combine the previous two theorems to show how the length of the delay line used to realize a sequential machine is bounded by the cycle lengths of that machine.

THEOREM 3.3 *Let $M = (Q, \Sigma, \delta)$ be a sequential machine and let q be a state of M which belongs to two distinct cycles of lengths m and n with $m > n$. Then, M cannot be realized, using a one-to-one assignment, by any* FSR *whose length is greater than or equal to $m + n - g$, where g is the greatest common divisor of m and n.*

Proof. We assume that M is realized, using a one-to-one assignment, by an FSR of length ℓ, where $\ell \geqslant m + n - g$. We denote the FSR state assigned to q by $(s_1, s_2, \ldots, s_\ell)$ and note that this state also belongs to cycles of lengths m and n. Using this ℓ-tuple, we form two infinite periodic sequences $\bar{x} = x_1x_2x_3 \cdots$ and $\bar{y} = y_1y_2y_3 \cdots$ as follows:

$$x_i = s_i \qquad \text{for} \quad i = 1, 2, \ldots, m,$$

and

$$x_i = x_{i-m} \qquad \text{for} \quad i \geqslant m + 1;$$
$$y_i = s_i \qquad \text{for} \quad i = 1, 2, \ldots, n,$$

and

$$y_i = y_{i-n} \qquad \text{for} \quad i \geqslant n + 1.$$

From the first part of Theorem 3.1, it follows that

$$(s_1, s_2, \ldots, s_\ell) = (x_1, x_2, \ldots, x_\ell) = (y_1, y_2, \ldots, y_\ell)$$

so that

$$x_i = y_i \qquad \text{for} \quad i = 1, 2, \ldots, \ell.$$

Now, since $\ell \geqslant m + n - g$, these two sequences satisfy the conditions of Theorem 2 and $x_i = x_{i+g}$ for $i \geqslant 1$. Hence, $s_i = s_{i+g}$ for $i = 1, 2, \ldots, \ell - g$.

But g is less than m and divides m which is a contradiction to the second part of Theorem 3.1. Hence ℓ must be less than $m + n - g$. Q.E.D.

We now show that $m + n - g$ is the best bound for which Theorem 3.3 holds. To this end, consider sequential machine M in Fig. 2. State A is in

Q \ Σ	0	1
A	A	B
B	C	D
C	B	A
D	D	C

FIG. 2. Sequential machine M.

a cycle of length 1 under input 0 and a cycle of length 3 under input sequence 101. Hence, Theorem 3.3 shows that M cannot be realized by a feedback shift register of length greater than 2. To see that it can be realized by one of length 2, consider the FSR in Fig. 3 and its state transition table in Fig. 4.

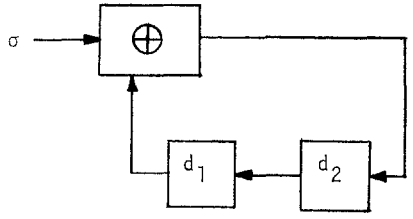

FIG. 3. Feedback shift register F.

	S^2 \ Σ	0	1
(A)	00	00	01
(B)	01	10	11
(C)	10	01	00
(D)	11	11	10

FIG. 4. State transition table for F.

It is clearly a realization of M under the indicated assignment.

Acknowledgment

The authors thank Dr. C. L. Liu for his suggestions which led to an improved version of this paper, particularly the proof of Theorem 3.2.

References

Davis, W. A. (1968), Single shift-register realizations for sequential machines, *IEEE Trans. Computers* **17**, 421–431.

Haring, D. R. (1966), "Sequential-Circuit Synthesis: State Assignment Aspects," MIT Press, Cambridge, Mass.

Johnson, D. L. and O'Keefe, K. H. (1968), The application of shift registers to secondary state assignments: Part I, *IEEE Trans. Computers* **17**, 954–965.

Liu, C. L. (1964), Sequential machine realizations using feedback shift registers, in "Proceedings of the Fifth Annual Symposium on Switching Circuit Theory and Logical Design," Institute of Electrical and Electronic Engineers, New York.

Martin, R. L. (1969), "Studies in Feedback-Shift-Register Synthesis of Sequential Machines," MIT Press, Cambridge, Mass.

Nichols, A. J. (1965), Minimal shift register realizations of sequential machines, *IEEE Trans. Electronic Computers* **14**, 688–700.

Yoeli, M. (1963), Counting with nonlinear binary feedback shift registers, *IEEE Trans. Electronic Computers* **12**, 357–361.